REMARKS/ARGUMENTS

Claims 39-52 are pending in the application. Claims 7, 9-12, 21, 23-26, 30, 35, 37 and 38 have been canceled. New claims 39-52 have been added. No new matter has been added.

Claims 7, 9-12, 21, 23-26, 30, 35, and 37 are rejected under 35 USC §103(a) as being unpatentable over Sudia (5,659,616) in view of Schneier et al. (5,956,404). Claim 38 is rejected under 35 USC §103(a) as being unpatentable over Schneier et al. (5,956,404) in view of Schneier et al. (5,978,475).

The claims have been canceled without prejudice or disclaimer and new claims 39-52 have been added. New claims 39-52 are directed to a digital signing method, a digital signing apparatus, and a computer program product for creating a digital signature.

The digital signature generation method of the present invention includes the following three steps: (1) computing a hash value of inputted data, (2) encoding the hash value into predetermined format data after adding padding data to the hash value as necessary, (3) encrypting the encoded data by using the private key.

In the present invention, inputted data include a message to be signed (M_N)and previous log data ($h(M_{N-1})$, $Sign_{N-1}$). A hash value of the inputted data including a message to be signed is computed (step 1). The computed hash value of the inputted data is encoded to produce encoded data of a predetermined format (step 2). Then, a secret key is applied to the encoded data to generate a digital signature (step 3). Support for these steps can be found throughout the specification, specifically on page 5, lines 15-24 and page 19, line 29 - page 20, line 1 of the originally filed specification.

According to one embodiment of the present invention, a secret key can be applied to either a previous data itself or a hash value of the previous data and to a hash value of a message to be signed. See page 20, line 16-22 of the specification.

Schneier et al. (US Patent No. 5,956,404) discloses a method for generating a new signature by using a previous signature data. In Schneier, the signing process is done through hashing the message and encrypting the hashed message by the private key. In order to ensure

that the encryption becomes extremely difficult to break, the hashed message is usually padded to increase the size of the package to be signed.

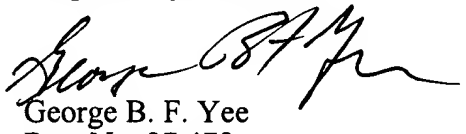
In Schneier, using the padded space, the auditing bits are put in the signature package. Thus, previous signature data is added to a padding space for padding of the hash value. However, in the present invention, the previous signature data is already included in data for computing hash value and so Schneier does not show this aspect of the invention.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



George B. F. Yee
Reg. No. 37,478

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
GBFY:gjs
60569556 v1